

AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0038] with the following amended paragraph:

[0038] The message digest extractor 404 extracts the received truncated message digest value 320 from the encrypted data packet 312. As explained above, the transmitted data 302 is padded then encrypted and finally reduced to its original size. Accordingly, the received encrypted data 302 is received de-padded encrypted payload 310 ~~data 320~~. The encrypted payload 310 is padded to the maximum size by the padding engine 424. The de-padded encrypted payload 310 ~~resulting padded encrypted data 302~~ is used to generate a message digest which is compared to the received message digest. In the exemplary embodiment, since the received message digest 320 is truncated, the locally generated message digest is truncated (truncated message digest value 426) before it is compared to the received truncated message digest value 420 by the message digest evaluator 410.

Please replace paragraph [0039] with the following amended paragraph:

[0039] After it is determined that the session count 332 is acceptable, the message digest generator 404 generates a message digest based on the complete (expanded) received session count, the received de-padded encrypted payload 310 ~~data 302 produced by the padding engine 424~~ and the message digest key 318.